

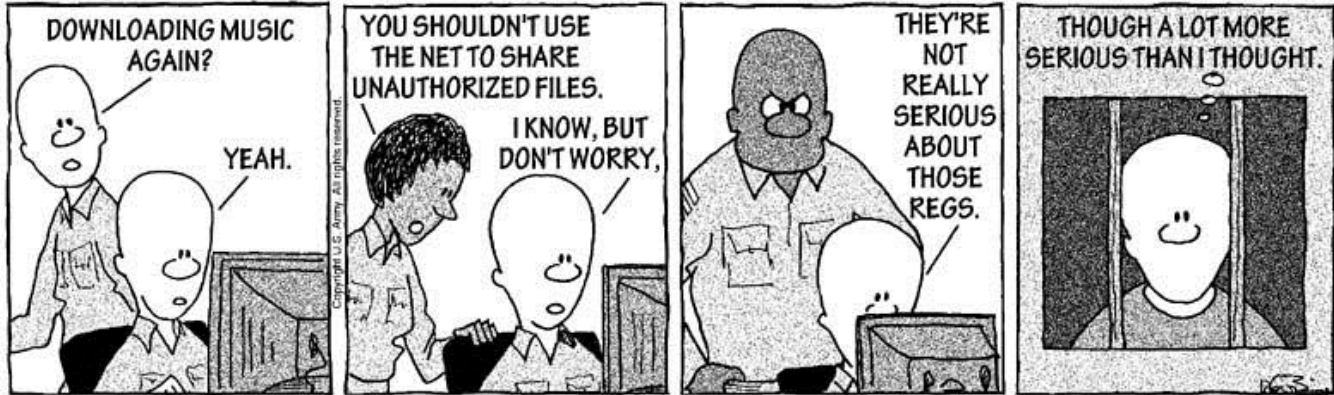
# Government Computer Misuse is Anything but Harmless Fun!

December 2005



## ON CYBER PATROL

As covered or mandated by AR 25-2



The next song you download may put your unit, your clearance, or your job (or life) at risk. Whether you are doing it from a newsgroup, illegal site or a legitimate music provider, it potentially unlocks the door for intruders. The same is true for other related activity. Unauthorized use or the installation of unapproved or illegal software invites system compromises.

Downloading music or videos, chatting, playing online games, or engaging in similar activities on a government computer is not only illegal use of government resources, but more importantly, it puts information and people at risk. What might seem like an innocent way to kill free time could allow spyware, aggressive malicious software or intruders directly into the system. This activity often requires downloading unauthorized software onto an Army computer, a clear violation of AR25-2. Installation of unauthorized Peer to Peer (P2P) applications is strictly forbidden and network monitoring is being conducted to identify illegal activities associated with users performing such activity.

This problem is widespread, even in the civilian world. Five major Internet companies have formed a coalition to put a stop to sites and advertisers that knowingly download spyware, adware, trackware and other malicious software. Federal and state laws are being enacted to address such activity as well. While annoying marketing companies generate most of this software development, some applications are capable of recording every keystroke and sending that information to unknown and often untraceable, entities. Industry sources estimate that approximately 91 percent of civilian computer users have made some modification to their systems to avoid this type of software. They do it to avoid ads; military personnel need to do it to protect our information and our forces.

Misuse of government equipment is a punishable offense. But that is not the only crime. More importantly the use of such subversive technologies exposes your computer, your network, your unit and yourself to cyber attacks, intrusions, and data exfiltration that could end up costing lives. If after you have downloaded the latest tune or selected your team for fantasy football, the way you log onto your computer, the next briefing you prepare, your sensitive personal information, or your unit's capabilities could be sent directly to a terrorist, hacker or insurgent group. This information is sent without any indications or warnings, and once sent can never be recovered.

How does that affect you? In perspective, 9.9 million individuals were affected by identity theft alone last year. That official document saved on your system may contain personal information such as your social security number that can be unknowingly shared as a result of the illegal software installation. Personal information is usually sold or traded in underground communities, and accounts or credit cards are rapidly established under your identity. Outcome: it will cost you thousands of dollars and potentially years to correct.

And if any download activity violates federal copyright laws it carries a secondary penalty.

The Army is taking this very seriously because of the potential harm to our forces. Every soldier must realize it is their duty to protect their fellow soldiers and not engage in unauthorized online activities. If you're involved in such activity, it's time to stop and think of the consequences.

Is an online game or a few new songs worth the risk?